

MTSA Regulations found at 33 CFR Subchapter H
Part 105--Facilities

Q. What facilities are affected by 33 CFR Part 105?

Ans. The regulations found in 33 CFR Part 105 apply to:

- Any U.S. facility subject to 33 CFR parts 126, 127, or 154.
- Facilities that receive vessels subject to SOLAS, 1974, chapter XI
- Foreign cargo vessels greater than 100 gross register tons except foreign vessels that have on board a valid International Ship Security Certificate certifying that the verifications required by Part A, Section 19.1, of the International Ship and Port Facility Security (ISPS) Code have been completed. See additional requirements in 33 CFR 104.105 (c).
- Facilities that receive vessels certificated to carry more than 150 passengers, except those vessels not carrying, embarking, or disembarking passengers at the facility
- Facilities that receive U.S. cargo vessels greater than 100 GRT, subject to 46 CFR Chapter I, Subchapter I, except facilities that only receive commercial fishing vessels inspected under 46 CFR part 105
- Barge fleeting facility that receives barges carrying, in bulk, cargoes that are regulated by 46 CFR Chapter I, Subchapters D or O, or Certain Dangerous Cargoes. See 33 CFR 105.105 and NVIC 03-03 Change-1.

Q. What is the impact to a facility owner/operator who is subject to the MTSA regulations of 33 CFR Part 105 and who fails to submit a required facility security plan and assessment package to the Coast Guard?

Ans. On or after July 1, 2004, a facility owner and/or operator subject to the MTSA regulations of 33 CFR Part 105 is required to have a U.S. Coast Guard approved facility security plan in order to conduct MTSA applicable operations. Failure to have fully implemented the approved facility security plan is a violation of the MTSA regulations and may result in a civil penalty against the owner/operator of the facility. Under the Regulations, the U.S. Coast Guard Captain of the Port (COTP) may impose civil penalties that range up to \$25,000.00 per violation of the MTSA requirements. After the July 1, 2004 deadline, non-compliant operators are subject to having their operation shut down until an approved security plan is in place. See 33 CFR 105.310, 33 CFR 105.410, 33 CFR 101.415 and NVIC 03-03 Change-1.

Q. What is the process for submission and approval of a Facility Security Plan (FSP)?

Ans. The owner or operator of a facility not in service on or before December 31, 2003, must submit a completed Facility Security Assessment (FSA) report, including a completed Coast Guard Vulnerability and Security Measures Summary (CG-Form 6025), one copy of their FSP, and a letter certifying that the FSP meets applicable requirements of this Part to the United States Coast Guard 60 days prior to beginning operations. The preferred method for submission is by email to the National Facility Plan Review Center (NFPRC) at NFSPPRC@BV.COM. Emailed documents must be sent in a password protected, zipped document. After emailing the document, the sender must call 1-866-377-8727 to confirm receipt and to provide the password for the document.

Other delivery methods may also be used such as U.S. Postal Service first class mail, regular parcel post, or by a delivery service, i.e. Federal Express, UPS, etc.). The FSP documents may be mailed in an electronic (CD) or paper format. Electronic versions (CD) should be sent by a delivery service to avoid radiation processing of the documents. All plan documents delivered via commercial carrier should be stamped with the Sensitive Security Information (SSI) warning statement and delivered using the SSI transmission procedures outlined in NVIC 9-02 Change-1. The outside of the document mailer is not to be marked with the SSI warning statement. It is strongly recommended that a Return Receipt be requested. The addressee label for carrier delivered documents is:

Black & Veatch Special Projects Corporation
Mailstop Q6, Attn: Security Officer
6601 College Boulevard
Overland Park, Kansas 66211.

Should an owner or operator submit their FSP documents directly to a cognizant COTP, the documents will be immediately forwarded by the COTP to the National FSP Review Center for processing.

If the owner or operator intends to operate under an approved Alternative Security Program (ASP), each facility must submit a letter via one of the options listed above, indicating which approved ASP the owner or operator intends to use and a completed Coast Guard Vulnerability and Security Measures Summary Form CG -6025. See 33 CFR 105.410, 33 CFR 105.310, and NVIC 03-03 Change-1.

Q. What is the Alternative Security Program (ASP) and who is eligible to participate?

Ans. The Alternative Security Program (ASP) means a third-party or industry organization developed standard that the Commandant, U. S. Coast Guard has determined provides an equivalent level of security to that established by 33 CFR Subchapter H. See 33 CFR 101.105

A facility owner or operator may use an Alternative Security Program (ASP) approved under 33 CFR Part 101.120 if the ASP is appropriate to that facility and the ASP is implemented in its entirety.

Q. What is the process for submission and approval of the Alternative Security Program (ASP)?

Ans. A maritime industry organization electing to use the facility ASP option must complete and submit the required information for review and approval to the U.S. Coast Guard Commandant (G-MP). See 33 CFR 101.120 (c) and 33 CFR 105.410.

A facility owner or operator intending to operate under an approved facility ASP must submit a letter signed by the facility owner or operator, to the cognizant CG COTP or the National Facility Plan Review Center (NFPRC) at:

Black & Veatch Special Projects Corporation
Mailstop Q6, Attn: Security Officer
6601 College Boulevard
Overland Park, Kansas 66211.

The letter should state which approved ASP the owner or operator intends to use and must include the U.S. Coast Guard Vulnerability and Security Measures Summary (CG -6025). See 33 CFR 105.410, Appendix A to Part 105, and NVIC 03-03 Change-1.

Q. What is the procedure for determining the status of a facility security plan review/approval?

Ans. The National FSP Review Center, located in Overland Park KS, will send an "acknowledgement of receipt" letter to the facility owner/operator who has submitted the required facility security plan documentation in accordance with the MTSA regulations of 33 CFR Part 105. The letter contains an assigned "Activity Number" that is required for the owner/operator to log-on electronically at <http://cgmix.uscg.mil/spr> to determine the status of their security plan submission.

If a facility owner or operator is unable to utilize the electronic access or has further questions, they should contact the National FSP Review Center at 1-866-FSP-USCG (1-866-377-8724).

Q. Are the MTSA Regulations applicable to a vessel that carries or a facility that handles Urea Ammonium Nitrate (UAN) Solution that contains ammonia (NH₃)?

Ans. UAN solution containing more than 2% NH₃

Any vessel that carries a UAN solution containing more than 2% NH₃ is required to be inspected pursuant to 46 CFR Subchapter O, Parts 151 or 153 and as a result, is regulated by 33 CFR 104.

Any facility that receives a vessel handling a UAN solution containing more than 2% NH₃ is subject to 33 CFR 105.

UAN solution containing 2% or less NH₃

Any vessel that carries a UAN Solution (2% or less NH₃) is not subject to 33 CFR 105 because UAN (2% or less NH₃) is an unregulated commodity when carried domestically unless another applicability factor of 33 CFR 104.105 applies to the vessel.

A facility that receives a UAN solution that contains 2% or less NH₃ from a vessel is subject to 33 CFR 105, regardless of whether the vessel is subject to MARPOL. A UAN solution that contains 2% or less NH₃ is classified as a category D noxious liquid substance by MARPOL regulations. 33 CFR 154 applies to any cargo that is listed as a category D noxious liquid substance. 33 CFR 154 does not limit its applicability to facilities receiving vessels subject to MARPOL and therefore, a facility handling a UAN solution that contains 2% or less NH₃ is subject to 33 CFR 105.

Q. How does a Public Access Facility (PAF) owner and/or operator apply for a Public Access Facility exemption per 33 CFR 105.110 (d)?

Ans. The guidance and procedures for the application, review, and granting PAF exemptions is published in the enclosures to NVIC 9-02, Change 2.

To ensure consistency, the USCG COTP will utilize the guidance found in NVIC 9-02, Change 2 to make the determination however, designation as a PAF does not constitute a total exemption of 33 CFR Part 105. See Policy Advisory Council Guidance 24-04 of March 25, 2004.

Q. Recently the U.S. Coast Guard determined that barges and facilities handling caustic soda solution are exempt from 33 CFR Part 104 unless another applicability factor is involved. This exemption has affected my ability to properly submit a vessel and/or facility security plan within the time period specified by the Regulations. Will the owner and/or operator be penalized for late submission?

Ans. The deadline for vessels and facilities handling caustic soda solution and affected by the change in policy as reflected in U.S. Coast Guard Policy Guidance is extended to September 1, 2004. See Policy Advisory Council Guidance 33-04, Change-1 of June 30, 2004.

Q. Does a facility owner or operator have to implement security measures for access control?

Ans. Yes, in general, the owner or operator of an MTSA regulated facility must ensure implementation of security measures to deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports. The facility owner or operator must also secure dangerous substances and devices that are authorized to be on the facility; and control access to the facility. See 33 CFR 105.255.

Q. How does a facility owner or operator handle access control measures with regards to official visits by law enforcement personnel?

Ans. 33 CFR 101.515(c) states “Vessel, facility, and OCS facility owners and operators must permit law enforcement officials in the performance of their official duties, who present proper identification in accordance with this Section, to enter or board that vessel, facility, or OCS facility at any time, without delay or obstruction. Law enforcement officials, upon entering or boarding a vessel, facility, or OCS facility, will, as soon as practicable, explain their mission to the Master, owner, or operator, or their designated agent.”

Facility owners/operators faced with any law enforcement official who declines to establish proper identity are encouraged to provide that official with a copy of the MTSA regulations and the relevant section on access control. If owners/operators have doubts about the authenticity of an official government identification document or credential or are concerned that denying access to an official may result in negative consequences, they should contact the cognizant U.S. Coast Guard COTP for guidance and assistance in effectively resolving the issue. See 33 CFR Part 104/105/106 and Coast Guard Policy Advisory #30-04 at <http://www.uscg.mil/hq/g-m/mp/mtsa.shtml> under “Policy Guidance.”

Q. What will Coast Guard facility inspectors be looking for when they visit a facility to conduct a compliance inspection to determine the status of implementation of the Facility Security Plan?

Ans. In general, Coast Guard inspectors will follow four key steps in determining the status of a facility owner or operator’s compliance with the approved Facility Security Plan (FSP). In conducting the inspection, the focus will be on determining that;

- The facility complies with its approved FSP;
- The approved FSP/ASP adequately addresses the requirements outlined in 33 CFR Part 105;
- The adequacy of the Facility Security Assessment and the completeness of the Facility Vulnerability and Security Measures Summary CG-6015; and

- The security measures in place adequately address vulnerabilities.

MTSA regulations do not mandate specific equipment or procedures but calls for performance-based criteria to be used to ensure security of the facility. MTSA places the responsibility to complete an accurate security assessment and to address the vulnerabilities in the Facility Security Plan on the owner or operator of the facility. The Coast Guard has the responsibility to verify that the facility is complying with its approved plan. Reference 33 CFR Part 105 and NVIC 03-03 Change 1, enclosures 10 and 11. Both documents are available via the internet at <http://www.uscg.mil/hq/g-m/mp/mtsa.shtml>.

Q. What is the impact to the operation of a facility if, as the result of a facility security plan compliance inspection, an owner or operator is found not to be operating in accordance with their approved FSP/ASP?

Ans. This type of deficiency is addressed using enforcement and compliance measures, ranging from lesser administrative actions (work lists, etc) up to and including more significant measures such as Notice of Violations, civil penalties, and operational controls that may restrict facility operations. For additional guidance refer to NVIC 03-03 Change 1, enclosures 10 and 11. The document is accessible via the internet at <http://www.uscg.mil/hq/g-m/mp/mtsa.shtml>.

Q. Where can an owner or operator find more specific guidance about compliance before a Coast Guard facility inspector arrives to conduct a MTSA-ISPS compliance inspection?

Ans. The Coast Guard maintains a broad range of MTSA-ISPS regulation and policy information that is easily accessible via the internet at <http://www.uscg.mil/hq/g-m/mp/mtsa.shtml>. If you are unable to find the desired information on the website, a Coast Guard "MTSA-ISPS Help Desk" is staffed from 8:00 AM-8:00 PM EST, Monday–Friday. The Help Desk staff can be reached at 1-877-687-2243 or 202-366-9991. References 33 CFR Part 105 and NVIC 03-03 Change 1 are also available on the internet site listed above.

Q. If a facility owner or operator is operating in accordance with the approved Facility Security Plan or Alternative Security Plan (FSP/ASP) but a Coast Guard facility inspector determines that a security measure(s) fails to adequately address an identified vulnerability, what is the procedure for requesting an amendment to the security plan? What actions will be required by the owner or operator in the interim?

Ans. A request to amend a previously approved FSP/ASP may be initiated by the cognizant COTP upon a determination that an amendment is needed to ensure a facility's security. The cognizant COTP will give the facility owner or operator written notice and request that the facility owner or operator propose amendments

addressing any matters specified in the notice. The facility owner or operator will have at least 60 days to submit the proposed amendment(s) to the cognizant COTP. Until amendments are approved, the facility owner or operator shall ensure temporary security measures are implemented to the satisfaction of the COTP. Reference 33 CFR Part 105.415 (a) (1).

Q. If a facility owner or operator, subsequent to having the FSP/ASP approved determines that an amendment to the security plan is necessary, what is the process for submission of the request? What actions will be required by the owner or operator in the interim?

Ans. If a proposed amendment to a previously approved FSP/ASP is initiated by a facility owner or operator, the request must be submitted to the cognizant COTP at least 30 days before the amendment is to take effect unless the cognizant COTP allows a shorter period for submission. The cognizant COTP will approve or disapprove the proposed amendment in accordance with 33 CFR Part 105.410. Until amendments are approved, the facility owner or operator shall ensure temporary security measures are implemented to the satisfaction of the COTP. Reference 33 CFR 105.415 (a) (2) & 33 CFR 105.410.

Q. Has a policy been published to outline procedures that Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and Transportation Security Agency (TSA) law enforcement personnel will follow in order to access vessels or facilities, other than during emergencies or exigent circumstances, in the performance of their duties?

Ans. A standardized policy outlining credentialing procedures for access to commercial vessel and entry to waterfront facilities, when law enforcement personnel are performing duties in the normal course of business, has been published. The full text of the policy, issued by the Undersecretary for Border and Transportation Security on August 24, 2004, can be found on this website under "Policy Guidance."

Recognizing that security is a shared responsibility with both the private and public sectors, CBP, ICE, and TSA law enforcement personnel should perform the following actions when attempting to access a commercial vessel or facility when performing their "normal" duties:

- (1) Identify yourself and organization verbally;
- (2) Present an official government issued photo identification card at each security checkpoint, being cognizant of protecting personal information (Ref: 33 CFR 101.515). There is no requirement to provide an alternate means of identification i.e. drivers license;
- (3) Explain, if necessary, that the ID card is federal property and therefore cannot and will not be surrendered;

- (4) Sign the visitor logbook, provide an office contact number if requested, and ensure that personal information (such as social security number) is not entered into the log;
- (5) Explain, if necessary, that properly identified law enforcement personnel on official business are not required to consent to a baggage or government vehicle search;
- (6) Explain, if necessary, that law enforcement personnel are authorized to carry firearms while conducting routine operations on a vessel or facility;
- (7) Recommend the facility or vessel amend their security plan if their approved security plan conflicts with the procedures outlined here for dealing with law enforcement officers; and
- (8) Accept a personnel escort, if an escort is readily available, and/or visitor badge if requested by the vessel or facility security representative. On those occasions in which law enforcement officials have specific safety or security concerns, law enforcement personnel may decline the offer of an escort.

These procedures shall not apply to law enforcement officers accessing vessels or facilities during emergencies or exigent circumstances in the performance of their duties.

U.S. Coast Guard personnel will follow similar credentialing procedures when attempting to access a commercial vessel or facility when performing their “normal” law enforcement duties. These procedures are published in U.S. Coast Guard Policy Advisory Council Decision (PACD) #30-04, “Credentialing of Federal, State and Local Officials,” issued 17 June 2004. A copy of PACD #30-04 can be found on the CG Intranet under ‘Policy Guidance’ at <http://cgweb.comdt.uscg.mil/G-Mp/Helpdesk.htm> or on the CG Internet under ‘Policy Guidance’ at <http://www.uscg.mil/hq/g-m/mp/mtsa.shtml>. For purposes of the MTSA, the applicability of the regulations to commercial vessels is specified in 33 CFR 104.105 and to waterfront facilities is specified in 33 CFR 105.105.